Incident Management

Description

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it is critical for an organization to have an effective means of managing and responding to them. The speed with which an organization can recognize, analyze, prevent, and respond to an incident will limit the damage done and lower the cost of recovery. This process of identifying, analyzing, and determining an organizational response to computer security incidents is called *incident management*.[1] The staff, resources, and infrastructure used to perform this function makeup the incident management capability.

Having an effective incident management capability in place is an important part of the deployment and implementation of any software, hardware, or related business process. Organizations are beginning to realize that communication and interactions between system and software developers and staff performing incident management activities can provide insights for building better infrastructure defenses and response processes to defeat or prevent malicious and unauthorized activity and threats.

This content area defines what is meant by incident management and presents some best practices in building an incident management capability. It also takes a look at one particular component of an incident management capability, a computer security incident response team (CSIRT) and discusses its role in the systems development life cycle (SDLC).

Overview Articles

Name	Version Creation Time	Abstract
Incident Management	11/14/08 3:00:07 PM	An incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract

1. Incident management in this article refers specifically to computer security incident management, not general problem management. A description of incident management can be found in the article "Incident Management" in this content area.

The Role of Computer Security Incident Response Teams in the Software Development Life Cycle	9/30/09 3:17:50 PM	This article describes one type of organizational entity that can be involved in the incident management process, a Computer Security Incident Response Team (CSIRT), and discusses what input such a team can provide to the software development process and what role it can play in the SDLC. CSIRTs in organizations performing software development and in related customer organizations may have valuable information to contribute to the life cycle. They may also be able to learn valuable information from developers concerning the criticality, operation, and architecture of software and system components that will help them identify, diagnose, and resolve computer security incidents in a more timely manner.
Defining Computer Security Incident Response Teams	11/14/08 3:01:11 PM	A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.
Incident Management	11/14/08 3:00:07 PM	An incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and

		procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Defining Computer Security Incident Response Teams	11/14/08 3:01:11 PM	A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.
Incident Management	11/14/08 3:00:07 PM	An incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

The Role of Computer Security Incident Response Teams in the Software Development Life Cycle	9/30/09 3:17:50 PM	This article describes one type of organizational entity that can be involved in the incident management process, a Computer Security Incident Response Team (CSIRT), and discusses what input such a team can provide to the software development process and what role it can play in the SDLC. CSIRTs in organizations performing software development and in related customer organizations may have valuable information to contribute to the life cycle. They may also be able to learn valuable information from developers concerning the criticality, operation, and architecture of software and system components that will help them identify, diagnose, and resolve computer security incidents in a more timely manner.